March

2013

MONTHLY
Cyber Security
Newsletter

Security Tips

Mississippi Department of Information Technology Services

Division of Information Security

Protect Yourself from Email Tax Scams

It's tax season and criminals are seizing the opportunity for scams. Don't become the next victim.

Scammers leverage every means at their disposal to separate you from your money, your identity, or anything else of value they can get. They may offer seemingly legitimate "tax services" designed to steal your identity and your tax refund, sometimes with the lure of bigger write-offs or refunds. Scams may include mocked up websites and tax forms that look like they belong to the IRS to trick you into providing your personal information.

Scam artists can prey on users by promising refunds that are fraudulent, a scam the IRS says has been rampant in previous years. In these scams, notices are posted on bulletin boards, in libraries, and at other community sites where people visit either in person or online. Scammers make money from this trick in two ways: first, they collect a fee for helping to "file" for a refund on behalf of their victims, and then they steal the victim's identity for further exploitation. The victims are left paying a fee for a fraudulent service, not getting a refund they thought they would, and are potentially in a position to face charges for failing to file a return or for committing fraudulent reporting.

How to Recognize an Email Tax Scam
According to the IRS, below are the key ways to recognize an email tax scam. The email:

- requests personal and/or financial information, such as name, SSN, bank or credit card account numbers or security-related information, such as mother's maiden name, either in the email itself or on another site to which a link in the email directs you;
- includes exciting offers to get you to respond, such as mentioning a tax refund or offering to pay you to participate in an IRS survey;
- threatens a consequence for not responding to the email, such as additional taxes or blocking access to your funds;
- has incorrect spelling for the Internal Revenue Service or other federal agencies;
- uses incorrect grammar or odd phrasing;
- discusses "changes to tax laws" that include a downloadable document (usually in PDF format) that purports to explain the new tax laws (these downloads are populated with malware that, once downloaded, may infect your computer).

Training Opportunities Coming Soon:

Web Application Security
March 18, 2013

ITIL Awareness
April 15, 2013

http://www.its.ms.gov/Services/Pages/Security-Training-Opportunities.aspx

this newsletter is brought to you by…

www.msisac.org

www.its.ms.gov

How To Avoid Becoming A Victim
To stay safer this tax season, follow these five steps:

1. **Secure your computer.** If your computer does not have proper security controls, it is vulnerable to access by criminals, who may be able to steal information stored on it. Make sure your computer has the latest security updates installed. Check that your anti-virus and anti-spyware software are running properly and are receiving automatic updates from the vendor. If you haven't already done so, install and enable a firewall.

2. **Carefully select the sites you visit.** Safely searching for tax forms, advice on deductibles, tax preparers, and other similar topics requires caution. Know the site. Know the company. Do not visit a site by clicking on a link sent in an email, found on someone's blog, or on an advertisement. The website you land on may look just like the real site, but it may be a well-crafted fake.

3. **Don't fall prey to email, web, or social networking scams.** Common scams tout tax rebates, offer great deals on tax preparation or offer a free tax calculator tool. If you did not solicit the information, it's likely a scam. ***If the email claims to be from the IRS, it's a scam – the IRS will not contact you via email, text messaging or your social network, nor does it advertise on websites.*** If the email appears to be from your employer, bank, broker, etc. claiming there is an issue with what they reported for you and you need to verify some information, it might be a scam. Do not respond to the email. Contact the entity directly before responding.

4. **Never send sensitive information in an email.** It may be intercepted and read by criminals.

5. **Use strong passwords.** Cyber criminals have developed programs that automate the ability to guess your passwords. To protect yourself, passwords must be difficult for others to guess, but at the same time, easy for you to remember. Passwords should have a minimum of nine characters and include upper case (capital letters), lowercase letters, numbers, and symbols. Make sure your work passwords are different from your personal passwords.

For More Information:
For additional information about tax related scams and identity theft, please visit:

- **Taxpayer Guide to Identity Theft:** www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft
- **Tax Scams/Consumer Alerts:** www.irs.gov/uac/Tax-Scams-Consumer-Alerts
- **IRS Releases the Dirty Dozen Tax Scams for 2012:** www.irs.gov/uac/IRS-Releases-the-Dirty-Dozen-Tax-Scams-for-2012
- **What's Hot –** IRS: www.irs.gov/uac/What's-Hot
- **Report Phishing:** www.irs.gov/uac/Report-Phishing